We claim:

1. A system for implementing a trusted counter in a personal communication device, comprising:

a secure module comprising a first storage device;

a second storage device;

a third storage device; and

a processor in communication with said secure module, said second and said third storage devices configured to:

execute authentication of said second storage device by said secure module;

request a counter value from second storage device to said secure module;

writing a secured state information and counter value from said secure module to said third storage device.

2. The system of claim 1, wherein said state information and counter value includes the number of failed attempts to correctly enter a PIN to gain access said personal communication device.

3. The system of claim 1, wherein said first storage device is a read-only memory device.

4. The system of claim 1, wherein said second storage device and said third storage device are external, read-write memory devices.

5. The system of claim 1, wherein said first and said second storage devices are tamper-resistant memory devices.

6. The system of claim 3, wherein said second storage device and said third storage devices are removable electronic card that is received by said personal communication device.

7. The system of claim 1, wherein the communication between said processor and said secure module, second storage device and third storage device comprises the execution of a plurality of protocols using an operating system of the personal communication device.

8. The system of claim 7, wherein said plurality of protocols are comprised of a create protocol, a read protocol, an update protocol.

9. The system of claim 1, wherein said third memory is an insecure storage device.

10. The system of claim 1, where said secured counter value is the counter value from said second storage device encrypted using a cryptographic transform.

11. The system of claim 1, wherein said personal communication device comprises a cellular telephone, a satellite telephone, a personal digital assistant or a bluetooth device.

12. The method for implementing a trusted counter in a personal communication device, comprising a first storage device within a secure module, a second storage device, and a third storage device, the method comprising:

authenticating a second storage device;

receiving a counter value from said second storage device to said secure module;

creating a secure state information and counter value in said second storage device using a cryptographic transform;

storing said secured counter value in said third storage device.

13. The method of claim 12, wherein said state information and counter value includes the number of failed attempts to correctly enter a PIN to access said personal communication device.

14. The method of claim 12, wherein said first storage device is a read-only memory device.

15. The method of claim 12, wherein said second storage device and said third storage device are read-write memory devices.

16. The method of claim 12, wherein said first storage device and said second storage device are tamper-resistant storage devices.

17. The method of claim 12, wherein said third storage device is an insecure storage device.

18. The method of claim 12, wherein the receiving said counter value from said second storage device is in response to a request from said second storage device.

19. The method of claim 12, wherein the personal communication device is a cellular telephone, a satellite telephone, a personal digital assistant or a bluetooth device.

20. A computer program product for implementing a trusted counter in a personal communication device comprising a first storage device within a secure module, a second storage device, and a third storage device, the method comprising:

a computer readable medium;

program code in said computer readable medium for authenticating second storage device;

program code in said computer readable medium for requesting a counter value from said second storage device;

program code in said computer readable medium for creating a secure state information and counter value in a second storage device based on said counter value from said first storage device; and

program code in said computer-readable medium for storing said secure counter value in a third storage device.

21. The computer program product of claim 20, wherein the program code for authenticating of said second storage device further comprises:

program code for receiving a compliance certificate and a public key from the second storage device; and

program code for verifying the authenticity of the compliance certificate.

22. The computer program product of claim 20, wherein the program code further comprises program code for receiving a success or failure indication from said third storage device.